
USAA®
THE USAA
EDUCATIONAL
FOUNDATION®
PERSONAL SAFETY
cybersecurity

our mission

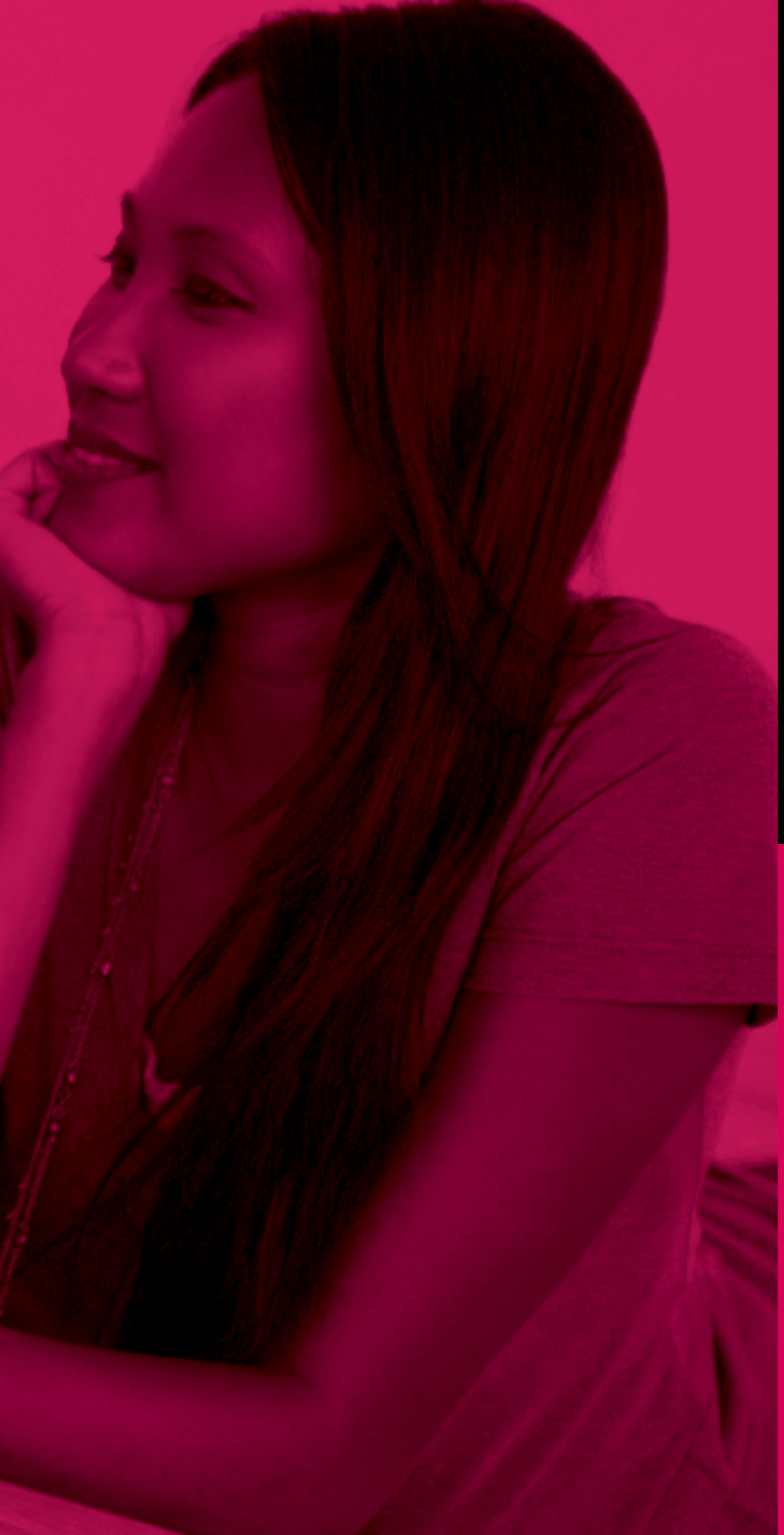
The mission of The USAA Educational Foundation is to help consumers make informed decisions by providing information on financial management, safety concerns and significant life events.

table of contents

cybersecurity & you

It's YOUR information

Financial institutions and other companies are required by law to protect your information. But you are your own best line of defense.



It's hard to imagine day-to-day life without the option of doing so many things online. You can transfer funds, pay bills and go shopping — from virtually anywhere.

But this kind of convenience can open the door to "cybercriminals" eager to steal money, personal information and even your identity. When this happens, it can take months or even years to clear your name, credit history and online reputation.

This information provides tips to protect you, your family and friends from cybercriminals.

Common **cybercrimes**

Fraud

Identity theft

Cyberstalking

Information warfare

Viruses and malware

safeguarding your privacy

Your digital subscriber line (DSL) or cable modem gives your computer continuous access to the Internet. Think of it as the front door to your home — you need to keep it secure to keep criminals out. You wouldn't open the door to just anyone, or distribute copies of your house key. The same discretion applies here.

Make this a **habit**	**Because**
Keep operating systems, application software and browsing tools up to date and set them to automatically install updates.	**They most likely provide your first defense against malware, viruses and other things that create damage or allow illegal access to your computer or network.**
Set your browser and your e-mail spam/junk filter to the medium or high security settings. Turn on your pop-up blocker. Never click on e-mail links from unknown or suspicious sources.	**This can protect against spam or phishing schemes. Spam is an unsolicited junk e-mail. Phishing is an unsolicited e-mail that pretends to come from a well-known company or even someone you know.**
Install and regularly update anti-virus and firewall protection on all computers that you own — even equipment that isn't Internet accessible.	**Unprotected devices can spread infection through the Internet, and also through USB drives and other removable media like your digital camera.**
Avoid using unfamiliar computers, mobile devices and networks, especially those provided in airports, hotels, Internet cafes and other public locations. Always log off from all websites that you use. Exercise caution when using public or free Wi-Fi networks, and avoid accessing bank accounts, e-mail or other sensitive accounts.	**Cybercriminals monitor these public computers and networks to capture user names and passwords.**
When using a wireless router device, check the owner's manual to securely set up your wireless network. For more information on using Wi-Fi networks visit *onguardonline.gov*	**This can keep cybercriminals from hacking into your system.**

passwords
equal protection

A password is a secret word used to confirm your identity when you log on to a website. Like the key to your home, you need to keep it safe.

Stronger password

Create passwords using a combination of at least eight letters and numbers, with both uppercase and lowercase letters. Adding special characters can increase the security of your passwords. Longer passwords are harder to decipher.

Memorable password

Think of a phrase or sentence meaningful to you and easy to remember. Then, take the first character from each word, alternate uppercase and lowercase and use some common letter-number substitutions.

Refresh your password

Change your password every 60 to 90 days to avoid the risk of cybercriminals gaining access to your personal information.

Phishing

Be skeptical of any e-mail or message that asks for confirmation of your username and password.

Personal information

Avoid using dictionary words. Never use personal information as part of your password, such as your name, pet or child's name, birthday, Social Security number or your current or former address.

Simple is not safe

Don't use simple letter or number patterns and sequences, such as "abcdefg" or "121212."

Never reuse passwords

Don't use the same password for every account or retail site, and never reuse passwords.

Don't store in devices

Don't store your password online or in documents or files on any mobile device — if the device is stolen, it gives the thief access to everything.

if it's personal, keep it private

Some people are fooled into revealing too much private information on the Internet because it seems safe, or they think they're acting anonymously. But sharing sensitive information — even photos and videos on social networks — can put you, your family and others at risk. Follow the same rules online as you would in the real world. If it's too much information, keep it to yourself.

Does your username give away too much?

NEVER USE:

- Your full name, home address or phone number.
- Names, addresses or phone numbers of family or friends.
- Your Social Security Number (SSN).
- Passwords or personal identification numbers (PINs).
- Credit card or bank account numbers.
- Your workplace or school.
- Previous addresses or historical information that could be used to identify you.

Close unused **accounts**

Have you ever opened a social networking account and then lost interest in it? It's a good idea to completely close any unused social networking accounts. Some social networking websites have established policies to delete, update, transfer or possibly preserve accounts, but their policies vary. There are even services available to help survivors manage a loved one's social networking accounts after their death. For specific instructions, contact the company directly.

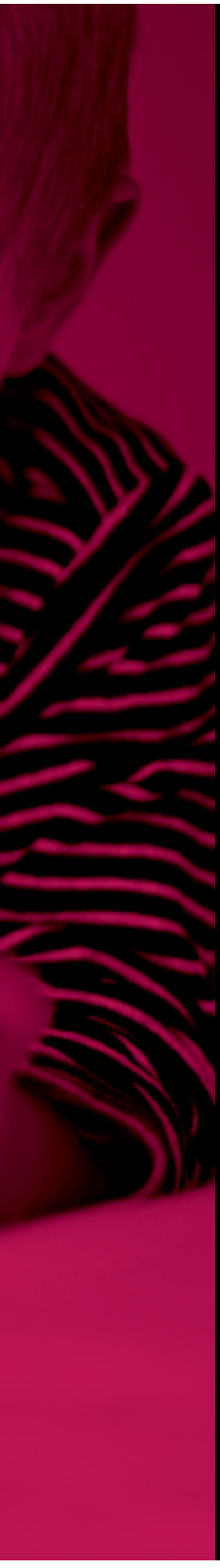
tips for safe social networking

- Never post that you are away from home or discuss current or future travel plans.
- Set your privacy settings to “friends only.”
- Keep your “friends” list short enough to manage. Know who you can trust to handle your news and photographs appropriately. Decline requests from people you don’t know personally.
- Before sending a message, consider how it could be read by others. Saying anything online that is cruel or damaging to someone’s reputation isn’t just rude, it’s also dangerous. It puts you at risk of being accused of slander or defamation, and could even escalate.
- Never allow anyone to photograph you in an embarrassing or compromising situation and don’t post anything that would cause you or others embarrassment or shame. You never know where these things will end up, and they could be used against you.
- Don’t forward another individual’s e-mail without permission.
- Keep in mind that posted information can be seen by anyone, not just your family and friends. Screen your posts as if you know they’ll be seen and judged by such people as your boss, potential employers, college admissions officers and law enforcement authorities.
- Check out the privacy policies and security provisions of social websites before engaging with them. Do they monitor or block inappropriate content? Do they make it easy to report potentially illegal or abusive content? If not, avoid using that site.
- Never share your full e-mail contact list with websites. This can lead to you and your contacts receiving spam and phishing e-mails.
- Never follow a link that asks you to log onto a social networking site. Links may lead to fake websites created to steal information or install malware.

protecting children while they are online

take action!

If you suspect your child is in danger contact law-enforcement authorities and the National Center for Missing & Exploited Children at *cybertipline.com*



Keeping your **child safe online**

If you have children, it's up to you to know what they are doing online so that you can guard them against the dangers that exist for unsuspecting minors.

- ☑ Set age-appropriate limits. Determine how much time per day your children can spend online. What social networking websites can they visit? Are chat rooms okay? Set rules and enforce them.
- ☑ Communication is the key to keeping children safe. Spend time talking with your children about their social networking activities. Ask them to tell you if they encounter someone or something online that makes them uncomfortable — especially if you suspect a child is at risk.
- ☑ Keep the computer in the family room or other busy areas of your home so it's easier to monitor their online activity.
- ☑ Keep up with their accounts and passwords, and randomly ask to view their profiles and postings.
- ☑ Many popular security software packages feature parental controls you can use to block inappropriate websites and content. You can also purchase stand-alone parental control and monitoring software.

Online predators

WARNING SIGNS THAT A CHILD MAY HAVE BEEN TARGETED:

- Uncharacteristic silence or withdrawal from the family.
- Turning off the monitor or reducing a Web page when you enter the room. If this is happening, log on to your child's computer and look for evidence of inappropriate websites. "Google" your child's name to see if his personal information is on the Internet.
- Spending a lot of time online — especially at night, when most predators are online.
- Making or receiving telephone calls to or from unrecognized numbers.

When to **take action**

Immediately contact law-enforcement authorities if your child has:

- Been asked for personal information, photographs or videos.
- Received obscene material from individuals or companies.
- Received misleading Internet links that point to websites containing harmful materials.
- Received threats to their life or safety or threats to others.

meeting an online friend

If you only know someone online, you don't really know them. Obviously, if any online conversation makes you uncomfortable in any way, you should log off immediately. But what if you want to meet an online acquaintance? Is it safe?

Before **you meet**

Frankly, it's never a good idea to meet up with someone you only know online. But if you choose to go through with it, be sure to take these precautions:

BEFORE YOU AGREE TO MEET:

1. Speak by phone — often, hearing an individual's voice and having a real conversation is revealing.
2. Learn as much as you can about them and verify that information.
3. Never share your home address.
4. Make arrangements to meet at a public place and arrive separately. If your online friend is a trusted individual, he will understand and welcome your caution. If your plan for a public meeting is met with objections, immediately terminate further conversation.

When **you meet**

1. Take along a trusted friend or family member or make sure they know where you are going, who you are meeting and how long you will be gone.
2. Check in with someone when you arrive and call when you are safely home.
3. Watch your alcohol intake. Do not leave a drink unattended.
4. Never leave with the individual. If you suspect you are being followed, drive to the nearest police station or public location for help.

cyberscams

Individuals misrepresent themselves online. Often the lies are harmless. Sometimes they aren't. It's very easy for cybercriminals to mislead potential victims over the Internet.

Links That Install Malware

An invitation to click on a link embedded in a photo, video, poll, game or quiz via text, e-mail or your social network site. The link prompts you to install a plug-in that installs malware on your computer which spreads quickly through the social network.

Comments On Your Post

A comment on your post that takes you to a phony login screen and asks for your username and password. The cybercriminal uses the information to break into your account.

Sexual Solicitation

A suggestive message, often imbedded in an explicit photo, inviting you to chat with or view photos of the sender. The link may direct you to an adult website asking for a credit card number and other personal information. The data could be used to commit identity theft and other crimes.

Send Money Now (419 Scam)

An e-mail message from a cybercriminal posing as a friend or loved one saying they have been robbed while traveling abroad. You are asked to wire money to an overseas account.

Charity Fraud

A cybercriminal asks for contributions to a fictitious charity supporting a sympathetic cause and offers to make a contribution on your behalf.

Celebrity Alerts

A message prompting you to download software to receive celebrity gossip. Malware is installed on your computer allowing the person to steal sensitive information.

Getting To Know You Quiz

A quiz asking seemingly innocent questions to "get to know you." Your answers are used to enter your financial accounts and steal your money.

IQ Tests

An online application for an IQ test requests your mobile phone number to send the results. Doing so enrolls you in a text messaging service that charges you monthly.

Advance Fee Schemes

A message or pop-up, asking you to pay upfront for an item or service you never receive.

Inheritance Fraud

An unsolicited message about an unclaimed family inheritance that asks you to send a fee to settle the nonexistent estate.

Internet Auction Fraud

You purchase an item and either do not receive it or receive something less than promised. You may be asked to pay using an untraceable wire service or an overseas address.

online harassment

Cybercriminals can use computer networks and devices to deliberately harass an individual or group by targeting victims through blogs, chat rooms, e-mail, instant messaging and social networking sites. If this happens to you, know what you're dealing with and how to take action.

To report an incident, contact the Federal Trade Commission (FTC) at *ftc.gov/ftc/contact.shtm* or the Internet Crime Complaint Center at *ic3.gov*

Types of **harassment**

Cyberstalking

- Ongoing, unwanted advances.
- May be threatening and could include disturbing and inappropriate or obscene content, including e-mails, text messages, photographs or spamming.

POTENTIAL HARM:
Can cause psychological trauma and often leads to real-life stalking and physical harm.

Take **action!**

Cyberstalking: Actions to take

- Report cyberstalking immediately to whoever owns the website.
- Send an e-mail to the offender warning that the contact is unwanted and tell them to stop.
- Keep a record of all contact made by the stalker, including dates, times, copies of all e-mails, postings or other communications.
- File a complaint with the stalker's Internet service provider (ISP) and your own ISP. Ask your ISP to block communications from the stalker.
- File a police report and include the details of each contact.
- Never agree to meet with a stalker for any reason.

Types of **harassment**

Cyberbullying

- The bully sends or posts messages or photographs intended to hurt or embarrass someone.
- The bully may be someone the victim knows or simply a stranger reacting to an Internet forum or social network post.

POTENTIAL HARM:

Cyberbullying can be more harmful and frightening than schoolyard bullying because it is more public. The bully can spread hurtful comments or innuendo and others may join in.

Online Impersonation

- Someone assumes your identity and uses your name or photographs and other identifying characteristics.
- Often enabled after you respond to a deceptive message.

POTENTIAL HARM:

The impersonator may clone your social networking site and post fake messages that appear to be from you.

Take **action!**

Cyberbullying: Actions to take

- Block all communication from the cyberbully and report the incident to your ISP. Stay offline, if necessary.
- Stay out of the chat room or other websites, and social networks frequented by the bully.
- Delete your current account and open a new one.
- Give your new e-mail address (or social website name) only to those you trust.

Online Impersonation: Actions to take

- If you receive a phishing e-mail or one you think is deceptive, don't reply.
- Immediately forward it to *spam@uce.gov*, where it enters an FTC database used to find and prosecute cybercriminals who send such messages.
- Notify your financial institution so they can investigate and protect your finances.

protecting your financial information

Treat your online PINs (personal identification number) and passwords as if they are cash. Don't leave them lying around where someone can take them. And make sure, when conducting business online, that the company is reputable and will keep your information and identity secure.

Military **personnel**

If you are an active duty servicemember away from your usual duty station, consider placing an "active duty alert" on your credit report. This requires creditors to verify your identity before issuing credit in your name. You only have to call one of the three consumer reporting agencies to place an alert and it will be activated by all three. The alert will remain in place for a full year. You will be removed from the marketing lists that offer credit and insurance for two years.

important factors:

Here are some good tips to follow when using your computer, mobile device or an automated teller machine (ATM) to electronically manage your banking:

Secure Your PINS

- Never store your PINs in your wallet or purse.
- Never share your PINs with anyone.
- Change your PIN at least every six months or when you are reissued a new debit card.

PIN Storage

- Consider what you want to happen in the event of sudden injury or death — and who needs to have convenient access to your PIN/password information.
- Consider storing your username, PINs and passwords in a secure location away from your residence, such as a safe deposit box at a bank or a safe in your attorney's office.
- Since some states restrict or limit access to a bank safe deposit box upon the death of the owner, consult with your legal adviser or financial planning professional to find the ideal balance of information security and access.

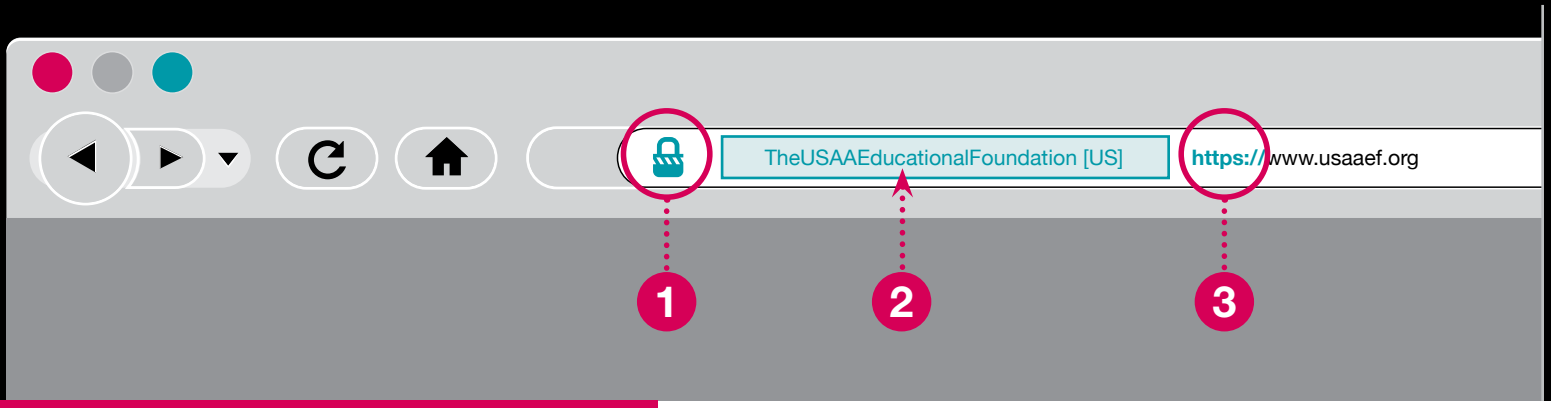
Check Your Credit Report

- Review your credit report at least annually; consider using a credit monitoring service.
- If it looks like your accounts have been compromised, immediately place a fraud alert on your credit report, requiring lenders to contact you before new credit accounts can be opened in your name.

Monitor Your Accounts

- If your financial institution offers you an online security token use it. (This is an electronic device or mobile application that generates a code or image to authorize access to a network service.)
- Frequently check activity on your bank, credit card and other financial accounts to make sure there are no unexplained charges or withdrawals.
- Enroll in any transaction-monitoring services provided by your bank.
- Ask your bank about registering any computers or mobile devices you use to access your accounts. They may be able to alert you, or require extra authentication, when an unregistered device attempts to access your accounts.

recognizing
a secured website



You can identify a secure website when you see the following indicators:

1 Padlock
Look for a closed padlock icon that indicates your transaction is being conducted over a secure connection.

2 Green Navigation Bar
High-security Web browsers display a green address bar indicating that the transaction is encrypted and the organization has been authenticated.

3 https://
If the website address begins with **https://**, your information will be encrypted during transmission.

Be sure, be secure

A secured site means your sensitive data is encrypted or coded before going out over the Internet so it can't be read by anyone else. Remember to always look for the icons and indicators shown on this page before entering or transmitting credit card numbers, checking account numbers or any other personal information.

mobile devices

Mobile devices — from smartphones to the latest tablets — are increasingly popular because they allow people to use the Internet almost anywhere. But this very mobility makes them an easy target for theft and cybercrime.

Global Positioning Systems (GPS)

Many mobile phones feature built-in Global Positioning Systems (GPS) that can help you find a place to eat, or help first-responders locate you if you're injured or too ill to place a call. That's a great feature. However, to defend against cybercriminals, you must take the same precautions as with your computer. In fact, the first line of defense is to keep your mobile devices — and all its stored data — from falling into the wrong hands.

Prevent unauthorized use

Build in safety measures that protect you if your mobile device is lost or stolen.

- Create a password that locks out or opens the keypad. Choose something easy for you to remember but difficult for others to guess.
- Turn on the auto-lock feature, which locks your mobile device after a period of inactivity.
- Activate the encryption feature, if available, to protect your personal information from anyone trying to gain access.
- Set up a remote-wipe capability. This allows you to remotely erase information stored on your mobile device, such as contact lists and e-mail.

Guard your **mobile devices**

Treat your smartphones and tablets as you would your wallet or purse — never leave them unattended, and keep them out of sight when not in use.

- Record account information for each device (make, model, serial number, password and contact list) and file this information in a secure location.
- Engrave a name or number on each device to clearly identify them as yours.
- Store only data to which you need quick and frequent access. Never store bank account numbers, SSNs, PINs, IDs, passwords or other sensitive information on a mobile device.
- Be cautious about allowing others to use your mobile devices, especially if you are enrolled in a mobile banking service. Never share your mobile phone number with strangers.
- Before recycling or disposing of any mobile device, erase or remove personal data and applications. If you aren't sure how to do this, consider seeking technical assistance.

When your mobile device is lost or stolen

Assume the worst if your phone or tablet goes missing.

- Contact your mobile service provider to remotely deactivate your account.
- If you've equipped your device with antitheft tools, use them to remotely track, erase or deactivate your data and file a police report.
- Notify your bank or credit card company if your mobile device contains financial information.
- Alert individuals on your contact lists that their information could be compromised.

Protect private information

Increasingly, criminals have the ability to access personal data on your mobile devices for malicious purposes. Use caution.

- Be careful who you share your mobile phone number with, and never share another individual's number without permission.
- Be cautious of the information you send in a text message and do not respond to text messages from a number you don't know.
- Never take or post photographs of others without their permission.
- Use caution when using social networking sites from your mobile device.

access more free educational materials today

can help you look out for the best interests of your family or an organization with free educational information.

- A Guide To Home Maintenance
- Basic Investing
- Behind The Wheel
- Estate Planning
- Life After The Military
- Making Your Home A Safer Place
- Suicide Prevention
- When Disaster Strikes: Readiness & Recovery

Visit ***usaaef.org*** to download digital versions or to order up to 250 printed copies of select publications or videos. Please call **(800) 531-6196** if you would like more than 250 copies. There is no charge for shipping. Some titles are not available in print.

THE USAA
EDUCATIONAL
FOUNDATION®

FOR MORE INFORMATION PLEASE VISIT:

usaaef.org

THE USAA EDUCATIONAL FOUNDATION®

This publication is not intended to be, and is not medical, safety, legal, tax or investment advice. It is only a general overview of the subject presented. The USAA Educational Foundation, a nonprofit organization, does not provide professional services for financial, accounting or legal matters. Applicable laws are complex, the penalties for non-compliance may be severe, and the applicable law of your state may differ. Consult your tax and legal advisers regarding your specific situation.

The USAA Educational Foundation does not endorse or promote any commercial supplier, product, or service. The Department of Defense, its military branches (Army, Marine Corps, Navy, Air Force and Coast Guard) and other governmental agencies do not endorse or favor any of the information, products or services contained in this publication.

70575-1014